BEFORE THE
CONSUMER FINANCIAL PROTECTION BUREAU

In the Matter of
Request for Information Regarding the Use of Mobile Financial Services by Consumers and Its Potential for Improving the Financial Lives of Economically Vulnerable Consumers

Docket No. CFPB-2014-0012

Comments of the Staff of the Bureau of Consumer Protection*

September 10, 2014

***These comments represent the views of the staff of the Bureau of Consumer Protection. They are not necessarily the views of the Commission or any individual Commissioner. The Commission has, however, voted to authorize the staff to submit these comments.**

I. INTRODUCTION

Federal Trade Commission (FTC or Commission) staff files this comment in response to the Consumer Financial Protection Bureau's (CFPB) June 12, 2014 Request for Information (RFI) seeking comment on the use of mobile financial services by consumers and economically vulnerable populations to access products and services, manage their finances, and achieve their financial goals.[1] In its RFI, the CFPB also seeks information about barriers to low-income, underserved, or economically vulnerable customers accessing mobile technology for financial services, as well as any potential consumer protection issues associated with the use of such technology.1

p-1(ue)4(s)-2(on)-2(o)4(to dy)20(vul(onom)-2dy)20(v(g)6(-2(con2(he)4(us)2(i)-2(t)-2d [(T(p)C15 Tw 172(om)-2(e)3(s)-pur
)401.14 128.48 57a4h, Tc 011.15 Tg235.32 405.c 128 T C15 Tal cons-2 (onom)-2n (onoh.15 Td [k)2(i)-2(t)-(e)4()-1(ub24(e)a

II. FTC AUTHORITY AND ACTIVITY IN THE AREA OF MOBILE COMMERCE

Beginning in 2002, the FTC has examined the benefits and consumer protection challenges associated with consumers' increasing use of mobile commerce. Through workshops,[5] reports,[6] and law enforcement actions,[7] the FTC has worked to ensure that consumer protections keep pace as mobile commerce transitions from concept to reality.[8] More recently, at its April 2012 workshop addressing mobile payments, *Paper, Plastic…or Mobile*, FTC staff convened experts with a range of perspectives to explore the consumer protection issues that arise in connection with mobile payments.[9] Following the workshop, FTC staff released a report in March 2013 (Mobile Payments Report) that highlighted the key areas for consumer concern discussed at the workshop, including the importance of clear disclosures about dispute resolution and liability limits and the need for mobile payment companies to provide greater transparency surrounding their data practices.[10] In particular, the report recognized the comparatively heavy use of mobile financial products by underbanked consumers.[11]

---

[5] *See Mobile Cramming: An FTC Roundtable*, FED. TRADE COMM'N (May 2013) (Workshop), *available at* http://www.ftc.gov/bcp/workshops/mobilecramming/

FTC staff has continued to make emerging mobile technology issues a priority by hosting

mobile payments.[18] FTC staff examined

B. Concerns About Unfair Billing Practices on Mobile Carrier Bills[27]

"Mobile carrier billing" – the ability to charge a good or service directly to a mobile phone account – is a payment method that offers many potential benefits for consumers who want to use their mobile phones to pay for goods and services.[28] In particular, carrier billing may be useful for consumers who do not have credit cards, or do not want to use them, especially for small transactions. In this way, carrier billing may be especially beneficial for unbanked and underbanked consumers.[29]

As carrier billing has developed, however, fraud has become a problem for consumers. In particular, mobile cramming – the unlawful practice of placing unauthorized third-party charges on mobile phone accounts – is a significant concern.[30] Mobile cramming occurs when consumers are signed up and billed for third-party services, such as ringtones and recurring text messages containing trivia or horoscopes, without their knowledge or consent. In six recent enforcement actions, the Commission has alleged that such practices have cost consumers millions of dollars,[31] and in three of these actions alone, defendants have agreed to orders imposing judgments totaling more than $160 million.[32]

In addition to the agency's enforcement actions, the Commission has engaged in policy and outreach initiatives to address mobile cramming issues. Specifically, the Commission convened a roundtable of interested stakeholders to discuss strategies to eliminate mobile

---

[27] The RFI seeks comment on the use of prepaid phones and carrier billing by underserved communities. RFI, s*upra* note 1, at 33733.
[28] MOBILE CRAMMING: AN FTC STAFF REPORT, *supra* note 7, at i.
[29] *Id.*
[30] *Id.*

cramming,[33] and FTC staff recently issued a report that recommends certain best practices for industry participants to protect consumers against mobile cramming.[34]

The report recommends that: (1) mobile carriers give consumers the option to block all third-party charges on their phone accounts; (2) market participants take appropriate action so that advertisements for products or services charged to a mobile bill are not deceptive; (3) market participants obtain consumers' express, informed consent to charges before they are billed to a mobile account, and maintain reliable records of such authorizations; (4) mobile carriers disclose all charges for third-party services clearly and conspicuously to consumers in a non-deceptive manner; and (5) carriers implement an effective dispute resolution process.[35]

Finally, the Commission has issued education materials on this topic encouraging consumers to check their mobile carrier bills carefully.[36]

C. Concerns About the Privacy of Consumers' Personal and Financial Data[37]

Another concern in the mobile environment is consumer privacy. The FTC has been the primary federal agency involved in privacy enforcement and policy since the 1970s, when it began enforcing one of the first federal privacy laws – the Fair Credit Reporting Ac-ghl.96 Td [(Cp)2(le)6(me)6

development; (2) offer more streamlined choices to consumers by providing choices at key decision-making moments and eliminating choices about obvious or expected data uses; and (3) make information collection and use practices more transparent.[40]

The Commission's work in this area has shown that mobile technologies raise unique privacy concerns due to the high number of companies involved in the mobile payments ecosystem and the large volume of data being collected. In addition to the banks, merchants, and payment card networks present in traditional payment systems, mobile payments often involve new actors such as operating system manufacturers, hardware manufacturers, mobile phone carriers, application developers, and coupon and loyalty program administrators.[41] When a consumer makes a mobile payment, any or all of these parties may have access to more detailed data about a consumer and the consumer's purchasing habits as compared to data collected when making a traditional payment.[42]

In its report, *Mobile Privacy Disclosures: Building Trust Through Transparency*,[43] FTC staff made a number of recommendations to improve transparency in the mobile environment, including recommendations that app developers provide "just-in-time" disclosures and obtain affirmative express consent from consumers prior to collecting sensitive information about consumers or sharing such sensitive data with third parties.[44]

FTC staff built on these recommendations in its recently-issued Mobile Shopping Apps Report. In addition to examining disclosures about the apps' liability and dispute procedures, discussed above, that report reviewed the privacy disclosures of mobile shopping apps, which included 30 in-store payment apps.[45] While most of the apps reviewed had privacy policies, staff found that those policies often used vague terms, reserving broad rights to collect, use, and share consumer data without explaining how the apps actually handled the information.[46] Staff recommended that companies clearly describe how they collect, use and share consumer data so that consumers can make informed choices about the apps they use.[47] Staff further recommended that consumers seek information before they download apps about how their data will be collected, used, and shared.[48] If consumers cannot find this information, or are

Law enforcement and education also have been critical to the FTC's efforts in this area. In the past several years, the FTC has brought a number of enforcement actions alleging deceptive and unfair conduct by mobile app developers in the collection or sharing of consumers' data,[50] including children's data.[51] Further, the FTC's website features many materials educating consumers about potential concerns related to mobile privacy.[52]

D. Concerns About the Security of Consumers' Personal and Financial Data

Mobile technologies also may raise security concerns. Indeed, consumers cite security concerns as one key reason for reluctance to use mobile devices for financial transactions.[53] As discussed at the FTC's workshop and report on mobile payments, technological advances in the mobile payment marketplace actually offer the potential for *increased* data security for financial information.[54] For example, mobile payment technology allows for encryption throughout the entire payment chain, often referred to as "end-to-end encryption."[55] However, as shown by FTC enforcement in this area, some industry players are not taking full advantage of the enhanced security features of mobile technologies.

The FTC is addressing mobile security through enforcement, policy initiatives, and consumer and business education. For example, in two recent cases against Fandango and Credit Karma, the FTC alleged that, despite their security promises, the companies failed to take reasonable steps to secure their mobile apps, leaving consumers' sensitive personal information at risk.[56] The complaints charged that Fandango and Credit Karma disabled a critical default process, known as SSL certificate validation, which would have verified that the apps' communications were secure. The FTC staff also issued educational material discussing how such apps may fail to provide security for their customers' data.[57]

---

[50] *See e.g. Snapchat, Inc.*, FTC File No. 132-3078 (F.T.C.

In 2012, the Commission issued warning letters to marketers of six mobile applications that provided background screening apps that they may be violating the FCRA.[65] The FTC warned the apps' marketers that, if they have reason to believe the background reports they provided were being used for employment screening, housing, credit, or other similar purposes, they must comply with the FCRA.[66] Further, the FTC settled charges last year with one enterprise that marketed its mobile apps as employment screening tools, alleging that the company operated as a consumer reporting agency without taking consumer protection measures required by the FCRA.[67]

In addition to raising issues under traditional data privacy laws like the FCRA, mobile services raise other data broker-related concerns. As noted above, the mobile ecosystem is unique in that there are many different entities and types of entities with the ability to access large volumes of potentially sensitive data. When data is sold to these entities, often outside the protections of specific privacy laws, questions arise regarding how this data may be used to either benefit or disadvantage low-income and underserved communities.

These concerns were discussed in a detailed study of the data broker industry that the FTC recently concluded. In May, the FTC issued *Data Brokers: A Call for Transparency and Accountability*, a report detailing staff's in-depth study of the practices of nine data brokers representing a cross-section of the industry.[68] The report notes that data brokers combine and analyze information about consumers to make inferences that can help companies prevent fraud, improve product offerings, and deliver tailored advertisements to consumers.[69] Further, data brokers make inferences about consumers and create data segments that group consumers based on the information they collect.[70] The inferences made about consumers can involve potentially sensitive information.[71] Indeed, the report found potentially sensitive categories to include those that primarily focus on ethnicity and income levels, such as "Urban Scramble" and "Mobile Mixer," both of which include a high concentration of Latinos and African Americans with low incomes.[72]

explore the potential uses of big data as well as the potential benefits and harms for particular populations of consumers.[74]

IV. CONCLUSION

FTC staff will continue to protect consumers in the mobile environment to ensure that this medium continues to grow and realize its full potential to benefit all consumers, including